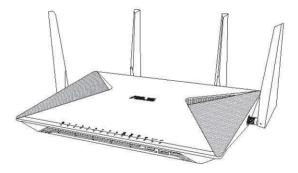
User Guide

BRT-AC828/M2 BRT-AC828

Wireless-AC2600 Dual WAN VPN Wireless Router





E11131 First Edition November 2015

Copyright © 2015 ASUSTeK Computer Inc. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Table of contents

1	Getting to know your wireless router
1.1	Welcome!
1.2	Package contents6
1.3	Your wireless router7
1.4	Positioning your router9
1.5	Setup Requirements
1.6	Router Setup11
	1.6.1 Wired connection11
	1.6.2 Wireless connection12
2	Getting started
2.1	Logging into the Web GUI 14
2.2	Quick Internet Setup (QIS) with Auto-detection
2.3	Connecting to your wireless network
3	Configuring the General settings
3.1	Using the Network Map 19
	3.1.1 Setting up the wireless security settings20
	3.1.2 Managing your network clients
	3.1.3 Monitoring your USB device
3.2	Creating a Guest Network
3.3	Using the USB Application28
	3.3.1 Using AiDisk
	3.3.2 Using Servers Center
	3.3.3 3G/4G
3.4	Using AiCloud 2.0
	3.4.1 Cloud Disk37
	3.4.2 Smart Access
	3.4.3 Smart Sync40

Table of contents

4	Config	guring the Advanced Settings	
4.1	Wirele	ess	41
	4.1.1	General	41
	4.1.2	WPS	43
	4.1.3	WDS (Bridge)	45
	4.1.4	Wireless MAC Filter	47
	4.1.5	RADIUS Setting	48
	4.1.6	Professional	49
4.2	LAN		51
	4.2.1	LAN IP	51
	4.2.2	DHCP Server	52
	4.2.3	Route	54
	4.2.4	IPTV	55
4.3	WAN		56
	4.3.1	Internet Connection	56
	4.3.2	Dual WAN	59
	4.3.3	Port Trigger	60
	4.3.4	Virtual Server/Port Forwarding	62
	4.3.4	DMZ	65
	4.3.5	DDNS	66
	4.3.6	NAT Passthrough	67
4.4	IPv6		68
4.5	VPN S	Server	69
4.6	Firew	all	70
	4.6.1	General	70
	4.6.2	URL Filter	70
	4.6.3	Keyword filter	71
	4.6.4	Network Services Filter	72
	4.6.5	IPv6 Firewall	73

Table of contents

4.7	Administration	74
	4.7.1 Operation Mode	74
	4.7.2 System	75
	4.7.3 Firmware Upgrade	
	4.7.4 Restore/Save/Upload Setting	77
4.8	System Log	78
5	Utilities	
5.1	Device Discovery	79
5.2	Firmware Restoration	80
5.3	Setting up your printer server	
	5.3.1 ASUS EZ Printer Sharing	81
	5.3.2 Using LPR to Share Printer	85
5.4	Download Master	90
	5.4.1 Configuring Bit Torrent download settings	91
	5.4.2 NZB settings	92
6	Troubleshooting	
6.1	Basic Troubleshooting	
6.2	Frequently Asked Questions (FAQs)	95
App	pendices	
Noti	ces	104
	-	

ASUS Contact information	118
Networks Global Hotline Information	119

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing an ASUS BRT-AC828/M2 Wireless Router! The ultra-thin and stylish BRT-AC828/M2 features 2.4GHz and 5GHz dual bands for an unmatched concurrent wireless HD streaming; SMB server, UPnP AV server, and FTP server for 24/7 file sharing; a capability to handle 300,000 sessions; and the ASUS Green Network Technology, which provides up to 70% powersaving solution.

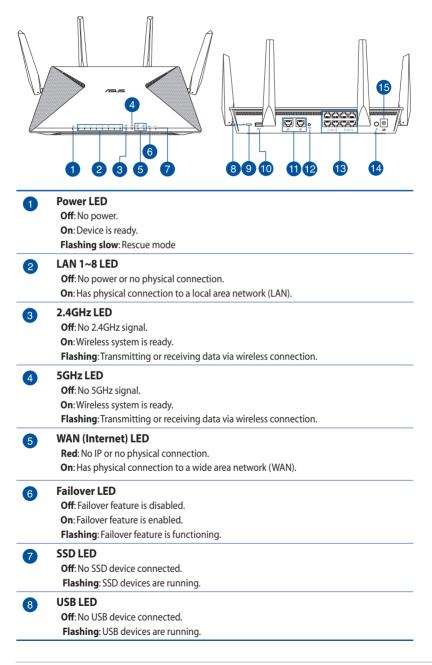
1.2 Package contents

- BRT-AC828/M2 Wireless Router
- ✓ Network cable (RJ-45)
- AC adapter
- Quick Start Guide

Support CD (Manual)

- If any of the items is damaged or missing, contact ASUS for technical inquiries and support, Refer to the ASUS Support Hotline list at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your wireless router



9	USB unmount button Press this button to safely remove the USB device.
10	USB 3.0 port Insert USB 3.0 devices such as USB hard disks or USB flash drives into this port.
1	WAN (Internet) ports Connect a network cable into these ports to establish WAN connection.
12	WPS button This button launches the WPS Wizard.
13	LAN 1 ~ 8 ports Connect network cables into these ports to establish LAN connection.
14	Power button Press this button to power on or off the system.
15	Power (DC-IN) port Insert the bundled AC adapter into this port and connect your router to a power source.

- Use only the adapter that came with your package. Using other adapters may damage the device.
- Specifications:

DC Power adapter	DC Output: +	DC Output: +19V with max 2.37A/3.42A current		
Operating Temperature	0~40°C	Storage	0~70°C	
Operating Humidity	50~90%	Storage	20~90%	

1.4 Positioning your router

For the best wireless signal transmission between the wireless router and the network devices connected to it, ensure that you:

- Place the wireless router in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- Keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at <u>http://www.asus.com</u> to get the latest firmware updates.
- To ensure the best wireless signal, orient the four detachable antennas as shown in the drawing below.



1.5 Setup Requirements

To set up your wireless network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/ 1000BaseTX)
- IEEE 802.11a/b/g/n/ac wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

- If your computer does not have built-in wireless capabilities, you may
 install an IEEE 802.11a/b/g/n/ac WLAN adapter to your computer to
 connect to the network.
- With its dual band technology, your wireless router supports 2.4GHz and 5GHz wireless signals simultaneously. This allows you to do Internet-related activities such as Internet surfing or reading/writing e-mail messages using the 2.4GHz band while simultaneously streaming high-definition audio/video files such as movies or music using the 5GHz band.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

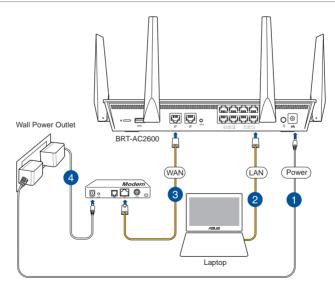
1.6 Router Setup

IMPORTANT!

- Use a wired connection when setting up your wireless router to avoid possible setup problems.
- Before setting up your ASUS wireless router, do the following:
 - If you are replacing an existing router, disconnect it from your network.
 - Disconnect the cables/wires from your existing modem setup. If your modem has a backup battery, remove it as well.
 - Reboot your cable modem and computer (recommended).

1.6.1 Wired connection

NOTE: You can use either a straight-through cable or a crossover cable for wired connection.



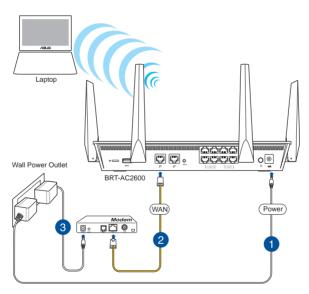
To set up your wireless router via wired connection:

1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.

2. Using the bundled network cable, connect your computer to your wireless router's LAN port.

IMPORTANT! Ensure that the LAN LED is blinking.

- 3 Using another network cable, connect your modem to your wireless router's WAN port.
- 4. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.



1.6.2 Wireless connection

To set up your wireless router via wireless connection:

- 1. Insert your wireless router's AC adapter to the DC-IN port and plug it to a power outlet.
- 2 Using the bundled network cable, connect your modem to your wireless router's WAN port.

- 3. Insert your modem's AC adapter to the DC-IN port and plug it to a power outlet.
- 4. Install an IEEE 802.11a/b/g/n/ac WLAN adapter on your computer.

- For details on connecting to a wireless network, refer to the WLAN adapter's user manual.
- To set up the security settings for your network, refer to the section Setting up the wireless security settings in Chapter 3 of this user manual.

2 Getting started

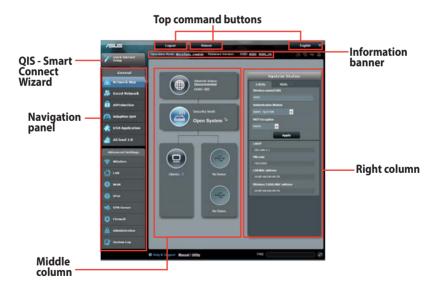
2.1 Logging into the Web GUI

Your ASUS wireless router comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Internet Explorer, Firefox, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

- 1. On your web browser, manually key in the wireless router's default IP address: <u>http://router.asus.com</u>.
- 2. On the login page, key in the default user name (**admin**) and password (**admin**).
- 3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



NOTE: If you are logging into the Web GUI for the first time, you will be directed to the Quick Internet Setup (QIS) page automatically.

2.2 Quick Internet Setup (QIS) with Autodetection

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

NOTE: When setting the Internet connection for the first time, press the Reset button on your wireless router to reset it to its factory default settings.

To use QIS with auto-detection:

1. Log into the Web GUI. The QIS page launches automatically.

	.168.50.1 is asking for your user name and password. The that it is from RT-AC 88U.
	r user name and password will be sent using basic n on a connection that isn't secure.
· · · · · · · · · · · · · · · · · · ·	
SV/	User name
	Password
	Remember my credentials
	OK

- By default, the login username and password for your wireless router's Web GUI is admin. For details on changing your wireless router's login username and password, refer to section 4.6.2 System.
- The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

2. The wireless router automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP** and **L2TP**. Key in the necessary information for your ISP connection type.

IMPORTANT! Obtain the necessary information from your ISP about the Internet connection type.

for Automatic IP (DHCP)



for PPPoE, PPTP and L2TP

Skip Setup Wizard	Account Setting	
Quick Internet Setup Check Connection Internet Setup Router Setup	Please enter your username and passeor User Name 2 Password 2 MAC Address(optional) 2	Asseed
	Enable VPN client Special Requirement from ISP	Uter Name 2 mmg
	Previous Next	Enter the user name and password for your internet connection information. These settings were given by your internet Service Previder (ISP).

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click Skip to manual setting and manually configure your connection settings.
- 3. Assign the wireless network name (SSID) and security key for your 2.4GHz and 5 GHz wireless connection. Click **Apply** when done.



- 4. Your Internet and wireless settings are displayed. Click **Next** to continue.
- 5. Read the wireless network connection tutorial. When done, click **Finish**.

Check Research Name (\$50) A508 Weakes Security Cyen System Internet Sectop Research Rem (\$50) A508 Weakes Security Cyen System Water Sectop Water Sectop Water Sectop Water Sectop UAN Note: 1253632314 UAN Note: 125363231 Note: 12536331 Note: 1253633 Note: 125363 Note: 1253633 Note: 1253633 Note: 1253633 Note: 1253633 Note: 125363 Note: 1253633 Note: 125363 Note: 12536 Note: 12536 Note: 12536 Note: 12536 Note: 1253 Note: 125 N	Quick Internet Setup	System Time: Mon, Feb 09 07: Wireless	59:03 2015 (PHT)	
Noternet Settup Noternet Kanna (\$\$10) A\$105_96 Scouler Setup Open Bystem WAN Open Bystem WAN Connection Type Aduratic IP WAN IP 192.164.52.174 LAN IP 192.163.50.1 MAC 69.05.41.26.59.1	Check Connection	Wireless Security		
Model or Solitop WAAN Addressite (P WAAN Connection Type Addressite (P WAAN (P 192.166.122.174 LAN P LAN (P 192.166.95.11 MAC 69.05.43.91.69.43	Internet Setup	Network Name (SSID)		
₩4AN 0P 112.568.123.174 LAN LAN 0P 112.188.50.1 MAX C 00.05.43.569.48	Router Setup			
MAC 50 0C-43 26 50-40		WAN IP		
	_		90 0C 43 26 68 48	
	_			

2.3 Connecting to your wireless network

After setting up your wireless router via QIS, you can connect your computer or other smart devices to your wireless network.

To connect to your network:

- 1. On your computer, click the network icon in the notification area to display the available wireless networks.
- 2. Select the wireless network that you want to connect to, then click **Connect**.
- 3. You may need to key in the network security key for a secured wireless network, then click **OK**.
- Wait while your computer establishes connection to the wireless network successfully. The connection status is displayed and the network icon displays the connected status.

- Refer to the next chapters for more details on configuring your wireless network's settings.
- Refer to your device's user manual for more details on connecting it to your wireless network.

3 Configuring the General settings

3.1 Using the Network Map

Network Map allows you to configure your network's security settings, manage your network clients, and monitor your USB device.



3.1.1 Setting up the wireless security settings

To protect your wireless network from unauthorized access, you need to configure its security settings.

To set up the wireless security settings:

- 1. From the navigation panel, go to **General** > **Network Map**.
- 2. On the Network Map screen and under **System status**, you can configure the wireless security settings such as SSID, security level, and encryption settings.

NOTE: You can set up different wireless security settings for 2.4GHz and 5GHz bands.

2.4GHz security settings



5GHz security settings



- 3. On the **Wireless name (SSID)** field, key in a unique name for your wireless network.
- 4. From the **Authentication Method** dropdown list, select the authentication method for your wireless network.

If you select WPA-Personal or WPA-2 Personal as the authentication method, key in the WPA-PSK key or security passkey.

IMPORTANT! The IEEE 802.11n/ac standard prohibits using High Throughput with WEP or WPA-TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11g 54Mbps connection.

5 Click **Apply** when done.

Ceneral <td

3.1.2 Managing your network clients

To manage your network clients:

- 1. From the navigation panel, go to **General** > **Network Ma**p tab.
- 2. On the **Network Map** screen, select the **Clients** icon to display your network client's information.
- 3. To block a client's access to your network, select the client and click the open lock icon.

3.1.3 Monitoring your USB device

The ASUS wireless router provides two USB ports for connecting USB devices or USB printer to allow you to share files and printer with clients in your network.



- To use this feature, you need to plug a USB storage device, such as a USB hard disk or USB flash drive, to the USB 3.0/2.0 ports on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the Plug-n-Share Disk Support List at <u>http://event.asus.com/networks/disksupport</u>
- The USB ports support two USB drives or one printer and one USB drive at the same time.

IMPORTANT! You first need to create a share account and its permission /access rights to allow other network clients to access the USB device via an FTP site/third-party FTP client utility, Servers Center, Samba, or AiCloud. For more details, refer to the section **3.5 Using the USB Application** and **3.6 Using AiCloud** in this user manual.

To monitor your USB device:

- 1. From the navigation panel, go to **General** > **Network Map**.
- 2. On the Network Map screen, select the **USB Disk Status** icon to display your USB device's information.
- 3. On the AiDisk Wizard field, click **GO** to set up an FTP server for Internet file sharing.

- For more details, refer to the section **3.5.2 Using Servers Center** in this user manual.
- The wireless router works with most USB HDDs/Flash disks (up to 4TB size) and supports read-write access for FAT16, FAT32, NTFS, and HFS+.

Safely removing the USB disk

IMPORTANT: Incorrect removal of the USB disk may cause data corruption.

To safely remove the USB disk:

- 1. From the navigation panel, go to **General** > **Network Map**.
- In the upper right corner, click > Eject USB disk. When the USB disk is ejected successfully, the USB status shows Unmounted.



3.2 Creating a Guest Network

The Guest Network provides temporary visitors with Internet connectivity via access to separate SSIDs or networks without providing access to your private network.

NOTE: BRT-AC828/M2 supports up to six SSIDs (three 2.4GHz and three 5GHz SSIDs).

To create a guest network:

- 1. From the navigation panel, go to **General** > **Guest Network**.
- 2. On the Guest Network screen, select 2.4Ghz or 5Ghz frequency band for the guest network that you want to create.
- 3. Click Enable.

The Gu		rnet connection for guests t	oud readhicts access to
	Fnable	Fnable	Enable
	Enable	Unable	Enable

- 4. To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
- 5. Assign a wireless name for your temporary network on the Network Name (SSID) field.

Guess Network			
	ist network can provide intern network.		
	ASUS_Guest1		
		Create	Create
	Limitless		
	Modify		
	ASUS_5G_Guest1		
		Create	Create
	Limitless		
	Modify		

- 6. Select an Authentication Method.
- 7. If you select a WPA authentication method, select a WPA Encryption.
- 8. Specify the Access time or choose Limitless.
- 9. Select **Disable** or **Enable** on the Access Intranet item.
- 10. When done, click **Apply**.

3.3 Using the USB Application

The USB Applications function provides AiDisk, Servers Center, Network Printer Server and Download Master submenus.

IMPORTANT! To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at <u>http://event.asus.com/2009/networks/disksupport/</u> for the file system support table.

3.3.1 Using AiDisk

AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

- 1. From the navigation panel, go to **General** > **USB application**, then click the **AiDisk** icon.
- 2. From the Welcome to AiDisk wizard screen, click Go.



3. Select the access rights that you want to assign to the clients accessing your shared data.



4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select I will use the service and accept the Terms of service and key in your domain name. When done, click Next.



You can also select **Skip ASUS DDNS settings** then click **Next** to skip the DDNS setting.

- 5. Click **Finish** to complete the setting.
- To access the FTP site that you created, launch a web browser or a third-party FTP client utility and key in the ftp link (ftp://<domain name>.asuscomm.com) you have previously created.

3.3.2 Using Servers Center

Servers Center allows you to share the media files from the USB disk via a Media Server directory, Samba share service, or FTP share service. You can also configure other settings for the USB disk in the Servers Center.

Using Media Server

Your wireless router allows DLNA-supported devices to access multimedia files from the USB disk connected to your wireless router.

NOTE: Before using the DLNA Media Server function, connect your device to the BRT-AC828/M2's network.

/SUS	Logout	Reboot	English 🔻
Quick Internet	Operation Mode: Wineless	router Firmware Version: SSID: ASUS ASUS_SG	9 8 @ 4 8
Setup	Hedia Server Network Place (1	Samba) Share / Cloud Disk FTP Share	
General	Media Server		5
品 Network Map	Set up the iTunes and DLNA med	la server.	
Suest Network	illines Server		
	Enable iTunes Server?	OFF	
AiProtection	Mida Server		
Maptive QoS	Enable DLNA Media Server		
1996	Media Server Name		
USB Application	Media Server Status		
AiCloud 2.0	Media Server Path Setting	O All Disks Shared Manual Media Server Path	
Advanced Settings		Apply	14

To launch the Media Server setting page, go to **General** > **USB application** > **Media Services and Servers** > **Media Servers** tab. Refer to the following for the descriptions of the fields:

- Enable iTunes Server?: Select ON/OFF to enable/disable the iTunes Server.
- Enable DLNA Media Server: Select ON/OFF to enable/ disable the DLNA Media Server.
- Media Server Status: Displays the status of the media server.
- Media Server Path Setting: Select All Disks Shared or Manual Media Server Path.

Using Network Place (Samba) Share service

Network Place (Samba) Share allows you to set up the accounts and permissions for the Samba service.

🥖 Setup	Media Server Network Place	(Samba) Share / Cloud Disk	FTP Share				
General	USB Application - Networ	k Place (Samba) Share	/ Cloud Disk				
Retwork Map	USB Application - Network Place (Samba) Share / Cloud Disk						
Suest Network	Enable Share	ON					
AiProtection	Allow guest login		OFF Username and pss sword is necessary to log in network place				
Adaptive QoS	Device Name						
🐇 USB Application	Work Group		NORKCROUP				
AiCloud 2.0	NTFS Sparse Files Support	Disable 📩					
Advanced Settings	Apply						
察 Wireless							
😭 LAN		Kouter Kingston OT 191 G2	R/W	R No			
💮 wan			Save Permission				

To use Samba share:

 From the navigation panel, go to General > USB application > Media Services and Servers > Network Place (Samba) Share / Cloud Disk tab.

NOTE: Network Place (Samba) Share is enabled by default.

2. Follow the steps below to add, delete, or modify an account.

To create a new account:

- a) Click 🕑 to add new account.
- b) In the **Account** and **Password** fields, key in the name and password of your network client. Retype the password to confirm. Click **Add** to add the account to the list.

Add new account lace(s	amba) Share / Cloud <mark>X</mark> D s				
New account has no read/write access rights.					
Account:					
Password:					
Retype password:					
	Add				
RT-AC66U					

To delete an existing account:

- a) Select the account that you want to delete.
- b) Click \varTheta.
- c) When prompted, click **Delete** to confirm the account deletion.

To add a folder:

- a) Click 🖳
- b) Enter the folder name, and click **Add**. The folder that you created will be added to the folder list.

The default access rights for a new folder is read/write.					
able Share with account Folder Name:					
Add					

- 3. From the list of folders, select the type of access permission that you want to assign for specific folders:
 - R/W: Select this option to assign read/write access.
 - R: Select this option to assign read-only access.
 - No: Select this option if you do not want to share a specific file folder.
- 4. Click **Apply** to apply the changes.

Using the FTP Share service

FTP share enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

IMPORTANT:

- Ensure that you safely remove the USB disk. Incorrect removal of the USB disk may cause data corruption.
- To safely remove the USB disk, refer to the section **Safely removing** the USB disk under 3.1.3 Monitoring your USB device.

/545	Logout	Reboot		English 🔻		
Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>ASUS ASUS.56</u> 🦞 🖧 🕞 🚓 🗈					
Setup	Media Server Network Place	(Samba) Share / Cloud Disk	TP Share			
General						
📇 Network Map	USB Application - FTP Share					
	Set the account and permission of FTP service.					
Guest Network	Enable FTP	ON				
	Allow anonymous login OFF Usemane and password is necessary to log in FTP service.					
Adaptive QoS	Maximum number of concurrent connections					
usil Application	Character set on FTP Server	UTF-4 •				
Aicloud 2.0	Apply					
Advanced Settings	$\odot \odot \oslash$					
💡 Wireless		Router	R/W R	No		
🚮 LAN			Save Permission			

To use FTP Share service:

NOTE: Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.5.1 Using AiDisk**.

- From the navigation panel, click General > USB application > Media Services and Servers > FTP Share tab.
- 2. From the list of folders, select the type of access rights that you want to assign for specific folders:
 - R/W: Select to assign read/write access for a specific folder.
 - W: Select to assign write only access for a specific folder.
 - **R**: Select to assign read only access for a specific folder.
 - No: Select this option if you do not want to share a specific folder.
- 3. If you prefer, you can set the **Allow anonymous login** field to **ON**.
- 4. In the **Maximum number of concurrent connections** field, key in the number of devices that can simultaneously connect to the FTP share server.
- 5. Click **Apply** to confirm the changes.
- To access the FTP server, key in the ftp link ftp://<hostname>.asuscomm.com and your user name and password on a web browser or a third-party FTP utility.

3.3.3 3G/4G

3G/4G USB modems can be connected to BRT-AC828/M2 to allow Internet access.

NOTE: For a list of verified USB modems, please visit: http://event.asus.com/2009/networks/3gsupport/

To set up 3G/4G internet access:

- 1. From the navigation panel, click **General** > **USB application** > **3G/4G**.
- 2. In the Enable USB Modem field, select Yes.
- 3. Set up the following:
 - Location: Select your 3G/4G service provider's location from the dropdown list.
 - **ISP**: Select your Internet Service Provider (ISP) from the dropdown list.
 - **APN (Access Point Name) service (optional)**: Contact your 3G/4G service provider for detailed information.
 - **Dial Number and PIN code**: The 3G/4G provider's access number and PIN code for connection.

NOTE: PIN code may vary from different providers.

- Username / Password: The username and password will be provided by the 3G/4G network carrier.
- **USB Adapter**: Choose your USB 3G / 4G adapter from the dropdown list. If you are not sure of your USB adapter's model or the model is not listed in the options, select **Auto**.
- 4. Click **Apply**.

NOTE: The router will reboot for the settings to take effect.

3.4 Using AiCloud 2.0

AiCloud 2.0 is a cloud service application that allows you to save, sync, share, and access your files.



To use AiCloud:

- 1. From Google Play Store or Apple Store, download and install the ASUS AiCloud app to your smart device.
- 2. Connect your smart device to your network. Follow the instructions to complete the AiCloud setup process.

3.4.1 Cloud Disk

To create a cloud disk:

- 1. Insert a USB storage device into the wireless router.
- 2. Turn on Cloud Disk.



3. Go to <u>https://router.asus.com</u> and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.

میں AiCloud	
Welcome. Who's coming home?	
Your Name.	
Your Password.	
⊙	

4. You can now start accessing Cloud Disk files on devices connected to the network.

NOTE: When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud for security reason.

admin Lasseyn 2014/11/08 (812/08 #	addwer: 101 101 1.00	English
ASUS AiCloud		
	Select an available device from the list on the left panel to start using AlCloud.	
1 sda1 [2.41 G8 / 7.46 G8]		
ANNEL_CHEN-NBL		
注 Setting C Refeat		ADJSTell Computer Inc. All rights reserve

3.4.2 Smart Access

The Smart Access function allows you to easily access your home network via your router's domain name.

AiCloud 2.0 Advanced Settings	Cloud Disk	Enables USB-attached storage devices to be accessed, streamed or shared through an internet-connected PC or device.
Wireless はAN 日本の	5	Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.
🚳 IPV6 🌾 VPN	Smart Sync	Enables synchronization of USB-attached storage with cloud services like <u>ASUS Webstorage</u> and other AlCloud 2.0-enabled networks.

NOTES:

- You can create a domain name for your router with ASUS DDNS. For more details, refer to section **4.3.5 DDNS**.
- By default, AiCloud provides a secure HTTPS connection. Key in <u>https://[yourASUSDDNSname].asuscomm.com</u> for a very secure Cloud Disk and Smart Access usage.

3.4.3 Smart Sync

/ISUS	Logout Reboot	English
V Quick Internet	Operation Mode: <u>Wireless router</u> Firmware Version: SSID: <u>ASUS ASUS SC</u>	8 @ +
semb	AiCloud 2.0 Smart Sync Server Settings Log	
General		
品 Network Map	AiCloud 2.0 - Smart Sync	
**		
Guest Network		
Guest Network	USBer	
AlProtection	http://aicloud-faq.asuscomm.com/aicloud-fa	
AlProtection Adaptive QoS CUSB Application	http://aicloud-faq.asuscomm.com/aicloud-fa	
AiProtection	http://aicloud-faq.asuscomm.com/aicloud-fa	1q/
AlProtection Adaptive QoS COB Application	http://aicloud-faq.asuscomm.com/aicloud-fa	1q/

To use Smart Sync:

- 1. Launch AiCloud, click **Smart Sync** > **Go**.
- 2. Select **ON** to enable Smart Sync.
- 3. Click Add new account.
- 4. Enter your ASUS WebStorage account password and select the directory that you want to sync with WebStorage.
- 5. Click **Apply**.

4 Configuring the Advanced Settings

4.1 Wireless

4.1.1 General

The General tab allows you to configure the basic wireless settings.

	Operation Mode: Mirelessinoste	🛫 Firmiware Version: SSID: ASUS ASUS 36 🦉 🖉 😓 😨 🔶 🖻
/ Setup	General WPS WDS Wireless	MAC Filter RADIUS Setting Professional
General	Wireless - General	
🐣 Network Map	Set up the wireless related information	below
🧟 Guest Network	Enabled Smart Connect	DIF.
AiProtection	Band	2.46Hz -
Adaptive QoS	850	
Mainter Traffic Analyzer	Hide SSID	• Yes O No
	Wireless Mode	Auto Colonical la Xuer 🖬 by Protection
dist Application	Channel bandwidth	20/40 мнг
AiCloud 2.0	Control Channel	AUTO
Advanced Settings	Edension Channel	Auto
	Authentication Method	NPA2-Personal
Wireless	WPA Encryption	ALS
🚮 LAN	WPA Pre-Shared Key	
😳 wan	Protected Management Frames	Disable
49 19v6	Network Key Rotation Interval	3600

To configure the basic wireless settings:

- From the navigation panel, go to Advanced Settings > Wireless > General tab.
- 2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
- 3. If you want to use the Smart Connect function, move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band 2.4GHz or 5GHz for optimal speed.

4. Assign a unique name containing up to 32 characters for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

NOTE: You can assign unique SSIDs for the 2.4 GHz and 5GHz frequency bands.

- 5. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
- 6. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
 - **Auto:** Select Auto to allow 802.11ac, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
 - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
 - **Legacy**: Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
- 7. Select the operating/control channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
- 8. Select the channel bandwidth to accommodate higher transmission speeds.
- 9. Select the authentication method.

NOTE: Your wireless router supports the maximum transmission rate of 54Mbps when the **Wireless Mode** is set to **Auto**.

10. When done, click **Apply**.

4.1.2 WPS

WPS (Wi-Fi Protected Setup) is a wireless security standard that allows you to easily connect devices to a wireless network. You can configure the WPS function via the PIN code or WPS button.



NOTE: Ensure that the devices support WPS.

To enable WPS on your wireless network:

- From the navigation panel, go to Advanced Settings > Wireless > WPS tab.
- 2. In the Enable WPS field, move the slider to ON.
- WPS uses 2.4GHz by default. If you want to change the frequency to 5GHz, turn OFF the WPS function, click Switch Frequency in the Current Frequency field, and turn WPS ON again.

NOTE: WPS supports authentication using Open System, WPA-Personal, and WPA2-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.

- In the WPS Method field, select Push Button or Client PIN code. If you select Push Button, go to step 4. If you select Client PIN code, go to step 5.
- 4. To set up WPS using the router's WPS button, follow these steps:
 - a. Click **Start** or press the WPS button found at the rear of the wireless router.
 - b.Press the WPS button on your wireless device. This is normally identified by the WPS logo.

NOTE: Check your wireless device or its user manual for the location of the WPS button.

- c. The wireless router will scan for any available WPS devices. If the wireless router does not find any WPS devices, it will switch to standby mode.
- 5. To set up WPS using the Client's PIN code, follow these steps:
 - a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.
 - b.Key in the Client PIN code on the text box.
 - c. Click **Start** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

4.1.3 WDS (Bridge)

Bridge or WDS (Wireless Distribution System) allows your ASUS wireless router to connect to another wireless access point exclusively, preventing other wireless devices or stations to access your ASUS wireless router. It can also be considered as a wireless repeater where your ASUS wireless router communicates with another access point and other wireless devices.



To set up the wireless bridge:

- From the navigation panel, go to Advanced Settings > Wireless > WDS tab.
- 2. Select the frequency band for the wireless bridge.

- 3. In the **AP Mode** field, select any of these options:
 - **AP Only**: Disables the Wireless Bridge function.
 - **WDS Only**: Enables the Wireless Bridge feature but prevents other wireless devices/stations from connecting to the router.
 - **HYBRID**: Enables the Wireless Bridge feature and allows other wireless devices/stations to connect to the router.

NOTE: In Hybrid mode, wireless devices connected to the ASUS wireless router will only receive half the connection speed of the Access Point.

- 4. In the **Connect to APs in list** field, click **Yes** if you want to connect to an Access Point listed in the Remote AP List.
- 5. By default, the operating/control channel for the wireless bridge is set to **Auto** to allow the router to automatically select the channel with the least amount of interference.

You can modify the **Control Channel** from **Advanced Settings** > **Wireless** > **General** tab.

NOTE: Channel availability varies per country or region.

 On the Remote AP List, key in a MAC address and click the Add button (1) to enter the MAC address of other available Access Points.

NOTE: Any Access Point added to the list should be on the same Control Channel as the ASUS wireless router.

7. Click **Apply**.

4.1.4 Wireless MAC Filter

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.

/ISUS	Logout	Reboot	English T
Quick Internet	Operation Mode: Wireless rout	ter Firmware Version: SSID: ASUS ASUS	<u>se</u> 8 ⊚ « 8
and p	General WPS WDS Wireless	HAC Filter RADIUS Setting Professional	
General	Wireless - Wireless MAC Filter	41844 - 10 - 145	
品 Network Map			
Suest Network		nl packets from devices with specified MAG address is	in your Wireless LAN.
	Basic Config Enable MAC Filer	O yes @ No	
AiProtection			
Maptive QoS	MAC Filler Mode	Accept	
USB Application	MAC filter list (Max Limit : 64)		
Use Application		MAG litter list	Add / Delete
AiCloud 2.0			Ð
Advanced Settings			
Wireless		Apply	
and a market	1		

To set up the Wireless MAC filter:

- From the navigation panel, go to Advanced Settings > Wireless > Wireless MAC Filter tab.
- 2. Tick Yes in the Enable Mac Filter field.
- 3. In the MAC Filter Mode dropdown list, select either Accept or Reject.
 - Select Accept to allow devices in the MAC filter list to access to the wireless network.
 - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
- 4. On the MAC filter list, click the **Add** 💿 button and key in the MAC address of the wireless device.
- 5. Click **Apply**.

4.1.5 RADIUS Setting

RADIUS (Remote Authentication Dial In User Service) Setting provides an extra layer of security when you choose WPA-Enterprise, WPA2-Enterprise, or Radius with 802.1x as your Authentication Mode.

/545	Logout	Reboot	English 🔻
Quick Internet	Operation Mode: Wireless rout	ter Firmware Version: SSID: ASUS ASUS 36	8 🗟 🗲 🛙
Setup	General WPS WDS Wireless	MAC Filter RADIUS Setting Professional	
General	Wireless - RADIUS Setting		
🔒 Network Map			
🧟 Guest Network		tional parameters for authorizing wireless clients through RADIUS of 'in "Winkess - General" as "WPA Enterprise/ WPA2 Enterprise	
	Frequency	2.4GHZ	
	Server IP Address		
Adaptive QoS	Server Port		
USB Application	Connection Secret		
AiCloud 2.0		Apply	
Advanced Settings			
🕎 Window			

To set up wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to WPA-Enterprise or WPA2-Enterprise.

NOTE: Please refer to section **4.1.1 General** section for configuring your wireless router's Authentication Mode.

- 2. From the navigation panel, go to **Advanced Settings** > **Wireless** > **RADIUS Setting**.
- 3. Select the frequency band.
- 4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
- 5. In the **Server Port** field, key in the server port.
- 6. In the **Connection Secret** field, assign the password to access your RADIUS server.
- 7. Click Apply.

4.1.6 Professional

The Professional screen provides advanced configuration options.

NOTE: We recommend that you use the default values on this page.

Dekk Seteraet	Courses where the states of rooting to	
	General MTS MDS Mindea N	AC Filter RADIUS Setting Professional
Concertal Notwork Map	Wireless - Professional	
Carst Network	Western Protectional Tailing allows you I successfy they been they are a stille on	i to net up withfilined personation for vehicles. The default values are escanoraided. Litter most more telline,
AlProtection	dimental di	2.600
	Crates Tade	0 Test # Sec
Adaptive (Jelli	Crain evens attacker	
USE Application	Claim in Courtre Placitie (seven dispit)	
AlCloud 7.0	Time of Day to Enable Radio	
	Dels is Dativ Radio (seenand)	
Advanced Artillage	Time of Day to Crudia Radio	
Hinters	Ser AP located	
3 i.m	Rearing statut	disate -
	Links CMP Drawing	alizable -
104	Material Tanglase)	Auto 1
	Prozentales Type	199
8 vin	AMPOU RTE	souls -
tires!	ATS Treastand	
Absistation	OTH Harver	
	Beauty Internet	
System Log	Enates 12 Burning	traffe 4
Network Looks	Enance Webbs APRO	that a
	Diseased interference management	studie -
	Reducing USE 3.8 ministering	Bruik te d
	Outinius AMPON appropriate	Brashle *
	Tartes GAM	Enemie -
	Capital Interferring	analia -
	Universal Descriptions	Anable
	To prever adjustment	
		Apply
	O Toly & Support Manual 10(0)	FNQ (P

In the **Professional Settings** screen, you can configure the following:

- **Frequency**: Select the frequency band that the professional settings will be applied to.
- Enable Radio: Select Yes to enable wireless networking. Select No to disable wireless networking.
- Date to Enable Radio (weekdays): You can specify which days of the week wireless networking is enabled.
- **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the week.

- Date to Enable Radio (weekend): You can specify which days of the weekend wireless networking is enabled.
- **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the weekend.
- Set AP isolated: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the router spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- AMPDU RTS:
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless router and 802.11g devices.

- **Enable WMM APSD**: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
- **TX Power adjustment**: TX Power adjustment refers to the milliWatts (mW) needed to power the radio signal output of the wireless router. Enter a value between 0 to 100.

NOTE: Increasing the TX Power adjustment values may affect the stability of the wireless network.

4.2 LAN

4.2.1 LAN IP

The LAN IP screen allows you to modify the LAN IP settings of your wireless router.

NOTE: Any changes to the LAN IP address will be reflected on your DHCP settings.

/545	Logout	Rebo	oot	6	nglish	
guick Internet	Operation Mode: Mireles	s roster	Firmware Version: SSID: ASUS ASUS_5G	8	6 €	
Śetup	LAN IP DHCP Server Ro	aute IPTV	Switch Control			
General		1. 1				
🔒 Network Map	LAN - LAN IP					
•	Configure the LAN setting of F	RT-AC3200.				
Guest Network	IP Address					
AiProtection	Subnet Mask					
Maptive QoS			Apply			
dist Application						

To modify the LAN IP settings:

- From the navigation panel, go to Advanced Settings > LAN > LAN IP tab.
- 2. Modify the IP address and Subnet Mask.
- 3. When done, click **Apply**.

4.2.2 DHCP Server

Your wireless router uses DHCP to assign IP addresses automatically on your network. You can specify the IP address range and lease time for the clients on your network.

1	Quick Internet	Operatio	on Mode: <u>Wire</u> l	less rout	er fi	imware Version:	SSID: ASUS ASUS_SG	8 6 4 8
1	Setup	LAN IP	DHCP Server	Route	IPTV	Switch Control		
	General	1000						
*	Network Map		DHCP Server					
22-	Guest Network	Carl #110	gn each client an	IP address	and info		automatic configuration used on IP n of DNS server IP and default gatewo <u>limit:32)_FAQ</u>	
Ô	AlProtection	Ranac G	antig	0010030000	694501905			
**	Adaptive QoS	Enable	the DHICP Server			🗢 Yes 🗢 No		
-		Router's	Oomain Name					
	USB Application	IP Pool	Starting Address					
2	AiCleud 2.0	IP Pool	Ending Address					
	dvanced Settings	LeaseT	îme					
	Wireless	Default	Gateway					
<u> </u>		DNS and	t WINS Server Set	ting		_	_	
୍ୟ	LAN	DNS Se	ner (
0	WAN	WINS S	erver					
63	IPv6	I ratie I	Manual A stageme	1		_		
		Enable	Manual Assignme	et		• Yes O No		
*	VPN Server	Mansak	y Assigned IP are	und the DH	.P list(bio	st. Nervalt: 323		_
D	Firewall		MAC ad	kiresa			IP Address	Add / Deloto
æ	Administration					*		Ð
-								
ها	System Log					App	ły	

To configure the DHCP server:

- From the navigation panel, go to Advanced Settings > LAN > DHCP Server tab.
- 2. In the Enable the DHCP Server field, tick Yes.
- 3. In the **Domain Name** text box, enter a domain name for the wireless router.
- 4. In the **IP Pool Starting Address** field, key in the starting IP address.

- 5. In the **IP Pool Ending Address** field, key in the ending IP address.
- 6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

NOTES:

- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.
- 7. In the **DNS and Server Settings** section, key in your DNS Server and WINS Server IP address if needed.
- 8. Your wireless router can also manually assign IP addresses to devices on the network. On the **Enable Manual Assignment** field, choose **Yes** to assign an IP address to specific MAC addresses on the network. Up to 32 MAC Addresses can be added to the DHCP list for manual assignment.

4.2.3 Route

If your network makes use of more than one wireless router, you can configure a routing table to share the same Internet service.

NOTE: We recommend that you do not change the default route settings unless you have advanced knowledge of routing tables.

guick Internet	Operation Mode: Wireless route	E Firmware Version:	SSID: ASUS ASUS SG	8648
Setup	LAN IP DHCP Server Route	IPTV Switch Control		
General	LAN - Route			
品 Network Map				
😹 Guest Network	This function allows you to add routing same connection to the Internet.	rules into Router. It is use	ful if you connect several routers	behind Router to share the
AiProtection	Basic Config Enable static routes	🗢 Yes 🔍 No		
💒 Adaptive QoS	Static Route List			
🚓 USB Application	Network/Host IP	Nelmask	Galeway Meb	ic Interface Add/Delete
A		-		LAN 🖸 💮
AiCloud 2.0				
Advanced Settings		App	ly l	
察 Wireless				

To configure the LAN Routing table:

- From the navigation panel, go to Advanced Settings > LAN > Route tab.
- 2. On the Enable static routes field, choose Yes.
- 3. On the **Static Route List**, enter the network information of other access points or nodes. Click the **Add** or **Delete** button to add or remove a device on the list.
- 4. Click **Apply**.

4.2.4 IPTV

The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.

/SLIS	Logout Rebo	ot	English 🔻
1 Quick Internet	Operation Mode: <u>Wineless router</u>	Firmware Version: SSID: ASUS ASUS SG	8 ⊕ ← 8
Setup	LAN IP DHCP Server Route IPTV	Switch Control	
General			
品 Network Map	LAN - IPTV		
2 Guest Network	To watch IPTV, the WAN port must be con- assigned to primary WAN.	ected to the Internet. Please go to <u>WAN - Dual WAN</u> to confi	im that WAN port is
AiProtection	Fort		
	Select ISP Profile	None	
Adaptive QoS	Choose IPTV STB Port	None	
disa Application	Special Applications		
AiCloud 2.0	Use DHCP routes	Hicrosoft	
AICIOUR 2.0	Enable multicast routing (IGMIP Proxy)	Disable +	
Advanced Settings	Enable efficient multicast forwarding (IGMP Snooping)	pisable	
💗 Wireless	UDP Proxy (Udpxy)		
		Apply	2

4.3 WAN

4.3.1 Internet Connection

The Internet Connection screen allows you to configure the settings of various WAN connection types.

Quick Internet	Operation Mode: <u>Wireless router</u>	Firmware Version: SSID: ASUS ASUS 36 🔠 🖓 🔶 🗇
Seeing	Internet Connection Port Trigger V	itual Server / Port Forwarding DMZ DDNS NAT Passtbrough
General		
🐣 Network Map	WAN - Internet Connection	
😹 Guest Notwork		WAN (wide area network). These types are selected from the dropdown menu beside fier depending on the connection type you selected.
AiProtection	Basic Config	
All-FoldCulon	WAN Connection Type	Automatic IP
Adaptive QoS	Enable WAN	© Yes ● No
usb Application	Enable NAT	O Yes 🖲 No
AiCloud 2.0	Enable UPsP UPsP EAD	O Yes O No
A CARGO DANA	WAN DNS Setting	
Advanced Settings	Connect to DNIS Server automatically	O Yes 🖷 No
Vireless	Account Setting	
🚮 LAN	Authentication	None
O WAN	Password	
	Special Requirement from ISP	
1Pv6	Host Name	
VPN Server	MAC Address	HAC Clone
🔽 Firewall		Apply

To configure the WAN connection settings:

- From the navigation panel, go to Advanced Settings > WAN > Internet Connection tab.
- 2. Configure the following settings below. When done, click **Apply**.
 - WAN Connection Type: Choose your Internet Service Provider type. The choices are Automatic IP, PPPOE, PPTP, L2TP or static IP. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
 - Enable WAN: Select Yes to allow the router Internet access. Select No to disable Internet access.

- Enable NAT: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- Enable UPnP: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- **Connect to DNS Server automatically**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- Host Name: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.

- MAC Address: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:
 - Contact your ISP and update the MAC address associated with your ISP service.
 - Clone or change the MAC address of the ASUS wireless router to match the MAC address of the previous networking device recognized by the ISP.
- **DHCP query frequency**: Changes the DHCP Discovery interval settings to avoid overloading the DHCP server.

4.3.2 Dual WAN

Your ASUS wireless router provides dual WAN support. You can set the dual WAN feature to any of these two modes:

- **Failover Mode:** Select this mode to use the secondary WAN as the backup network access.
- Load Balance Mode: Select this mode to optimize bandwidth, minimize response time and prevent data overload for both primary and secondary WAN connections.

/ISUS	Logout	leboot	English 🔫
Quick Internet Setup	Operation Mode: Wireless rout	er Firmware Version: SSID: ASUS ASUS 5G	a 5 € a
General	Internet Dual Connection WAN WAN - Dual WAN	Port Virtual Server / Port DMZ DDNS Trader Forwarding	NAT Passthrough
🥂 Guest Network			
AlProtection	Basic Config		1
Adaptive QoS	Enable Dual WAN	ON	
SUSB Application	Primary WAN Secondary WAN	usa 🖸	
Aicloud 2.0	Dual WAN Mode	Fail over	
Advanced Settings	Ping Time Watch Dog		-
👕 Windess	Interval	5 seconds	
🚮 lan	Delay Fail Count	8 seconds	
💮 wan	Enable Watch Dog	• Yes O No	
🚳 1Риб	2	Apply	

4.3.3 Port Trigger

Port range triggering opens a predetermined incoming port for a limited period of time whenever a client on the local area network makes an outgoing connection to a specified port. Port triggering is used in the following scenarios:

- More than one local client needs port forwarding for the same application at a different time.
- An application requires specific incoming ports that are different from the outgoing ports.

/ISUS	Logout		Reboot				English
14 Quick Internet	Operation Mode: 1	viceless	router Firmw	are Version:	SSID: ASUS A	5815_56	8 6 - 1
Setup	Internet Connection	Dual WAN	Port Trigger	Virtual Se Forwa		DMZ DDNS	NAT Passthrough
General						1000 - 00	225
船 Network Map	WAN - Port Trigg	ger					
🧟 Guest Network	Port Trigger allows yo two methods for open the time and devices	ning incoming	g data ports: port fo	rwarding and po	rt trigger. Part forwa	rding opens the s	pecified data ports a
AiProtection	access to the bigger forwarding allows mu						
Maptive QoS	port. Port. Trigger FA	a i					
USB Application	Basic Config		_	_			
	Enable Port Trigger		• Ye	s O No			
AiCloud 2.0	Well-Known Applicati	ons			•		
Advanced Settings	Trigger Part List (Max Limit :	32)			_	
😵 Wireless	Description		Trigger Port	Protocol	Incoming Port	Protocol	Add / Delete
				тер		TCP	Ð
C LAN				No data in t	ati)r.		
() WAN				Apply			

To set up Port Trigger:

- From the navigation panel, go to Advanced Settings > WAN > Port Trigger tab.
- 2. On the Enable Port Trigger field, tick Yes.
- 3. On the **Well-Known Applications** field, select the popular games and web services to add to the Port Trigger List.

- 4. On the **Trigger Port List** table, key in the following information:
 - **Description**: Enter a short name or description for the service.
 - **Trigger Port**: Specify a trigger port to open the incoming port.
 - **Protocol**: Select the protocol, TCP, or UDP.
 - **Incoming Port**: Specify an incoming port to receive inbound data from the Internet.
 - Protocol: Select the protocol, TCP, or UDP.
- 5. Click the **Add** 💮 to enter the port trigger information to the list. Click the **Delete** 🗿 button to remove a port trigger entry from the list.
- 6. When done, click **Apply**.

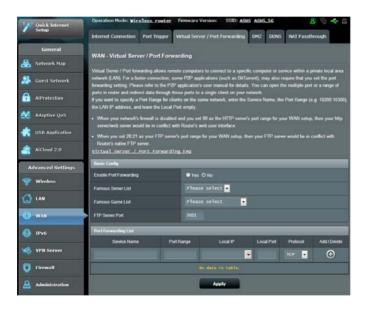
NOTES:

- When connecting to an IRC server, a client PC makes an outgoing connection using the trigger port range 66660-7000. The IRC server responds by verifying the username and creating a new connection to the client PC using an incoming port.
- If Port Trigger is disabled, the router drops the connection because it is unable to determine which PC is requesting for IRC access. When Port Trigger is enabled, the router assigns an incoming port to receive the inbound data. This incoming port closes once a specific time period has elapsed because the router is unsure when the application has been terminated.
- Port triggering only allows one client in the network to use a particular service and a specific incoming port at the same time.
- You cannot use the same application to trigger a port in more than one PC at the same time. The router will only forward the port back to the last computer to send the router a request/trigger.

4.3.4 Virtual Server/Port Forwarding

Port forwarding is a method to direct network traffic from the Internet to a specific port or a specific range of ports to a device or number of devices on your local network. Setting up Port Forwarding on your router allows PCs outside the network to access specific services provided by a PC in your network.

NOTE: When port forwarding is enabled, the ASUS router blocks unsolicited inbound traffic from the Internet and only allows replies from outbound requests from the LAN. The network client does not have access to the Internet directly, and vice versa.



To set up Port Forwarding:

- From the navigation panel, go to Advanced Settings > WAN > Virtual Server / Port Forwarding tab.
- 2. On the Enable Port Forwarding field, tick Yes.

- 3. On the **Famous Server List** field, select the type of service you want to access.
- 4. On the **Famous Game List** field, select the popular game that you want to access. This item lists the port required for your selected popular online game to work properly.
- 5. On the **Port Forwarding List** table, key in the following information:
 - Service Name: Enter a service name.
 - **Port Range**: If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty. Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,3021).

NOTES:

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with the router's web user interface.
- A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.
 - Local IP: Key in the client's LAN IP address.

NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **4.2 LAN** for information.

- Local Port: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
- Protocol: Select the protocol. If you are unsure, select BOTH.
- 5. Click the **Add** 💮 to enter the port trigger information to the list. Click the **Delete** 🗿 button to remove a port trigger entry from the list.
- 6. When done, click **Apply**.

To check if Port Forwarding has been configured successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

4.3.4 DMZ

Virtual DMZ exposes one client to the Internet, allowing this client to receive all inbound packets directed to your Local Area Network.

Inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. In a DMZ configuration, one network client receives all inbound packets.

Setting up DMZ on a network is useful when you need incoming ports open or you want to host a domain, web, or e-mail server.

CAUTION: Opening all the ports on a client to the Internet makes the network vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.

To set up DMZ:

- From the navigation panel, go to Advanced Settings > WAN > DMZ tab.
- 2. Configure the setting below. When done, click **Apply**.
 - IP address of Exposed Station: Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.

To remove DMZ:

- 1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
- 2. When done, click **Apply**.

4.3.5 DDNS

Setting up DDNS (Dynamic DNS) allows you to access the router from outside your network through the provided ASUS DDNS Service or another DDNS service.

/ISUS	Logout		Reboot			-	English	
Territ Quick Internet	Operation Mode: 1	tireless	router firm	ware Version: SSID	ASUS ASUS	56	8 6 4	Ē
Setup	Internet Connection	Dual WAN	Port Trigger	Virtual Server / Po Forwarding	rt DMZ	DONS	NAT Passthrough	
General								
Retwork Map	WAN - DDNS							
🚨 Guest Network		Idress, throu		ce that allows network clie iomain name. The wireles:				
AlProtection				Paddress (192,168 = =, 1 t and ODNS service cann				
Adaptive QoS	Enable the DDNS CI	ient	• 1	'es O No				
USB Application				Apply				
AiCloud 2.0								

To set up DDNS:

- From the navigation panel, go to Advanced Settings > WAN > DDNS tab.
- 2. Configure the following settings below. When done, click **Apply**.
 - **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
 - Server and Host Name: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).
 - If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.

• **Enable wildcard**: Enable wildcard if your DDNS service requires one.

NOTES:

DDNS service will not work under these conditions:

- When the wireless router is using a private WAN IP address (192.168. x.x, 10.x.x.x, or 172.16.x.x), as indicated by a yellow text.
- The router may be on a network that uses multiple NAT tables.

4.3.6 NAT Passthrough

NAT Passthrough allows a Virtual Private Network (VPN) connection to pass through the router to the network clients. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough and RTSP Passthrough are enabled by default.

To enable / disable the NAT Passthrough settings, go to the **Advanced Settings** > **WAN** > **NAT Passthrough** tab. When done, click **Apply**.

nsus	Logout		Reboot				-	English	
Quick Internet	Operation Mode: 🖌	irelesse	ester Firmw.	are Version:	SSID: ASU	S ASUS_	56	8 6 -	
Setup	Internet	Dual	Port Trigger		irver / Port ardino	DMZ	DONS	NAT Passthrough	1
General	Striction								
Network Map	WAN - NAT Pass	through							
	Enable NAT Passthro		a Virtual Private N	rtwork (VPN) c		as through			
Goest Network	PPTP Passbrough		Enal	ile 💌					
AiProtection	L2TP Passtrough			ile •					
Adaptive QoS	IPSec PassBrough			ile 💌					
USB Application	RTSP Passthrough			1e •					
	H.323 Passbrough			ile 💌					
AiCloud 2.0	GIP Passterough			ile •					
Advanced Settings	Enable PPPoE Relay			ble 🚪					
😵 Wineless				Apply					
😭 lan									
() WAN									

4.4 IPv6

This wireless router supports IPv6 addressing, a system that supports more IP addresses. This standard is not yet widely available. Contact your ISP if your Internet service supports IPv6.

/ISUS	Logout	Reboot	English
Vick Internet Setap	Operation Mode: Kircless rowt	er Firmware Version: SSID: ASUS ASUS_SG	8 6 4 8
General	IPv6		
🞎 Guest Network	Configure the IP46 Internet setting of F 1P46_EAQ	louter.	
AlProtection	Basic Cools	Disable •	
Adaptive QoS	Auto Configuration Setting		
🔹 USB Application	Enable Router Advertisement	Enable 👤	
AiCloud 2.0		Apply	

To set up IPv6:

- 1. From the navigation panel, go to **Advanced Settings** > **IPv6**.
- 2. Select your **Connection Type**. The configuration options vary depending on your selected connection type.
- 3. Enter your IPv6 LAN and DNS settings.
- 4. Click **Apply**.

NOTE: Please refer to your ISP regarding specific IPv6 information for your Internet service.

4.5 VPN Server

VPN (Virtual Private Network) provides a secure communication to a remote computer or remote network using a public network such as the Internet.

NOTE: Before setting up a VPN connection, you would need the IP address or domain name of the VPN server you are trying to access.

/ISUS	Logost	Reboot		English 🔻
Cuick Internet Setup	Operation Mode: <u>Wirele</u>	ss router Firmware Version	a: SSID: <u>Asus Asus s</u>	
General				100 CO. 100 CO.
🐣 Network Map	VPN Server - PPTP		PPTP.	OpenVPII
Suest Network	Easic Config			
	Enable VP% Server			
AlProtection	VPN Details		•	
Maptive QoS	Network Place (Samba) Supe	port Ves O No		
SB Application	To use the VPN server Plea			
AiCloud 2.0	(1) Enable the PPTP VPN se (2) Set the IP pool for client I (3) Set up the username and	P. (Maximum 10 clients) I password for VPN client.		
Advanced Settings		n program on your computer or smar onnection and the VPN server addres		
💎 Wireless	(6) If your WAN IP address • <u>VPN_Server_EAQ</u>	is dynamic, <u>please click h</u> a	ere to set the DONS,	
🚮 LAN	Username and Passworth (N	Aes Lamit : 16)		
🚯 wan	Connection Status	UserName	Password	Add/Delete
🔒 1Pv6				Ð
VPN -		App	Hy	

To set up access to a VPN server:

- 1. From the navigation panel, go to **Advanced Settings** > **VPN Server**.
- 2. On the Enable VPN Server field, select Yes.
- 3. On the **VPN Details** dropdown list, select **Advanced Settings** if want to configure advanced VPN settings such as broadcast support, authentication, MPPE Encryption, and Client IP address range.
- 4. On the Network Place (Samba) Support field, select Yes.
- 5. Enter the user name and password for accessing the VPN server. Click the 💿 button.
- 6. Click **Apply**.

4.6 Firewall

The wireless router can serve as a hardware firewall for your network.

NOTE: The Firewall feature is enabled by default.

4.6.1 General

To set up basic Firewall settings:

- From the navigation panel, go to Advanced Settings > Firewall > General tab.
- 2. On the Enable Firewall field, select Yes.
- 3. On the **Enable DoS protection**, select **Yes** to protect your network from DoS (Denial of Service) attacks though this may affect your router's performance.
- 4. You can also monitor packets exchanged between the LAN and WAN connection. On the Logged packets type, select **Dropped**, **Accepted**, or **Both**.
- 5. Click **Apply**.

4.6.2 URL Filter

You can specify keywords or web addresses to prevent access to specific URLs.

NOTE: The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

To set up a URL filter:

- From the navigation panel, go to Advanced Settings > Firewall > URL Filter tab.
- 2. On the Enable URL Filter field, select Enabled.
- 3. Enter a URL and click the 💮 button.
- 4. Click Apply.

4.6.3 Keyword filter

Keyword filter blocks access to webpages containing specified keywords.

/sus	Logout	Reboot		English 🔻
Quick Internet	Operation Mode: Wireless	router Firmware Version:	SSID: ASUS ASUS_SG	8 @ ← ≞
and a	General URL Filter Keyword	Filter Network Services Filter	IPv6 Firewall	
General				
🔒 Network Map	Firewall - Keyword Filter			
Suest Network	Keyword Filter allows you to block Limitations of the filtering function		containing the specified keyword	
AiProtection	1. Compressed webpages tha 2. Https webpages cannot be	t use HTTP compression technolo filtered.	gy cannot be filtered. <u>See . her e</u>	for more details.
Maptive QoS	Basic Config			
USB Application	Enable Keyword Filter	Enabled O Disabi	led	
	Keyword Filter List			
AiCloud 2.0		Keyword Filter List		Add / Delete
Advanced Settings				Ð
😴 Wireless				
😭 I.M		Apply		

To set up a keyword filter:

- From the navigation panel, go to Advanced Settings > Firewall > Keyword Filter tab.
- 2. On the Enable Keyword Filter field, select Enabled.

- 3. Enter a word or phrase and click the **Add** button.
- 4. Click **Apply**.

NOTES:

- The Keyword Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the Keyword Filter.
- Web pages compressed using HTTP compression cannot be filtered. HTTPS pages also cannot be blocked using a keyword filter.

4.6.4 Network Services Filter

The Network Services Filter blocks LAN to WAN packet exchanges and restricts network clients from accessing specific web services such as Telnet or FTP.

/545	Logout Rebe	et	English *
Wick Internet	Operation Mode: Wireless rowter	Firmware Version: SSID: ASUS ASUS_SG	9 8 Q 4 B
Setup	General URLTIMer KeywardTiller	Network Services (Bar DVG Firewall	
General	Firewall - Network Services Filter	0	
🐣 Network Hap			
🤼 Guest Network	services	to WAN packet exchanges and reshicts devices from	
AProtection	For example, if you do not want the device 80 will be blocked Lowve the source IP field blank to apply this	to use the Internet service, key in 80 in the declination I rule to all LAN devices.	port. The Ineffic Heat uses port
Maptive QuS	Black List Duration : During the scheduled the specified duration, all the clients in LAN	duration, clients in the Illack List carriest use the speci can access the specified retwork services.	lied network services. After
🔆 USB Application		I duration, clients in the White List care CMLY was the s Nile List and other network clients will not be able to a	
AiCheud 2.0	A DESCRIPTION OF THE REPORT OF T		
Advanced Settings	Affaring The Sector and provide allowed in	The second second	
🐨 Wireless	Retwork Services Filter		
100 C	Enable Network Services Filter	• Yes O No	
🞧 LAN	Filter latin type	mlack stor +	
😳 WAN	Web Known Applications	user Defined	
8 1946	Date to Cruble LAN to WAN Filter	Sitter Sitter Sitted Sitter Site	
	Time of Day to Enable LAN to WAN Filter		
VFN	Date to Enable LAN to WIN Filter		
C Howald	Time of Day to Enable LAN to WAN Filter		
Administration	Fillered ICMP packet types		
System Log	Network Services Filter Table (Max L) Source IF Port Range	eerit 22) Deskuster P Part Ranae Pr	and Add/Detete
2 Retwork Tools		Demonster Protocoge Pro	
		er data in table.	
		Assily	
	O this & Support Manual Likiby	FAQ	1.00

To set up a Network Service filter:

- From the navigation panel, go to Advanced Settings > Firewall > Network Service Filter tab.
- 2. On the Enable Network Services Filter field, select Yes.
- 3. Select the Filter table type. **Black List** blocks the specified network services. **White List** limits access to only the specified network services.
- 4. Specify the day and time when the filters will be active.
- 5. To specify a Network Service to filter, enter the Source IP, Destination IP, Port Range, and Protocol. Click the 💿 button.
- 6. Click **Apply**.

4.6.5 IPv6 Firewall

By default, your ASUS wireless router blocks all unsolicited incoming traffic. The IPv6 Firewall function allows incoming traffic coming from specified services to go through your network.

/ISUS	Logout	Reb	oot			inglish 🔻
Quick Internet	Operation Mode:	Wireless router	Firmware Version:	SSID: ASUS ASUS_SG	8	© ⊷ ≞
Quick Internet Setup	General URL Filt	ter Keyword Filter	Network Services Filter	IPv6 Firewall		
General						
📇 Network Map	Firewall - IPv6 F	irewall				
Suest Network	All outbound traffic o must be specifically		on your LAN is allowed, as	well as related inbound traff		bound traffic
AIProtection	You can leave the re for example)	emote IP empty to allow	v traffic from any remote hos	it. A subriet can also be spi		
Adaptive QoS	Basic Config					
Se module day	Enable IPv6 Firewal		O Yes @ No			
usb Application	Famous Server List		Please select 📕			
AiCloud 2.0	Indonesid Pereventil Re	des (Max Limit : 126)		_	_	
	Senice Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
Advanced Settings					тер	Ð
					Transmission in case	
💝 Wireless						

4.7 Administration

4.7.1 Operation Mode

The Operation Mode page allows you to select the appropriate mode for your network.

/645	Logout Roboot	English 🔫
V Quick Internet	Operation Mode: <u>wireless router</u> Femware Version: SSID: ASUS ASUS_SG	8648
< setup	Operation Mode System Firmware Upgrade Restore/Save/Upload Setting	
General		
🐣 Network Map	Administration - Operation Mode	_
🎎 Guest Network	Router supports several operation modes to meet different requirements. Please select the mode that ma	ich your situation.
AiProtection	Wireless router mode (Default) Access Point(AP) mode Media brid	
💒 Adaptive QoS	In werkens router IP sharing mode, Rovier connects to the Internet Au IPPPUE, DHCP, PPIPI, LZTP, or DBAS, wireless network to LAN clearls or devices. In Bas mode, NAT, Brewall, and DHCP server are analised by def Dynamic CMI are supported for DOHD and home usars. Select that mode if you are a first-free user or you.	will UPriP and
dis Application	any wire diversitata readera.	
aiCloud 2.0		
Advanced Settings		
💎 Wireless		
😭 lan		
💮 WAN		
4 19v6	Save	

To set up the operating mode:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Operation Mode** tab.
- 2. Select any of these operation modes:
 - Wireless router mode (default): In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.
 - Access Point mode: In this mode, the router creates a new wireless network on an exising network.
 - **Media Bridge**: This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via ethernet.

3. Click Apply.

NOTE: The router will reboot when you change the modes.

4.7.2 System

The **System** page allows you to configure your wireless router settings.

To set up the System settings:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
- 2. You can configure the following settings:
 - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
 - Time Zone: Select the time zone for your network.
 - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
 - Enable Telnet: Click Yes to enable Telnet services on the network. Click No to disable Telnet.
 - Authentication Method: You can select HTTP, HTTPS, or both protocols to secure router access.
 - Enable Web Access from WAN: Select Yes to allow devices outside the network to access the wireless router GUI settings. Select No to to prevent access.

- Allow only specified IP address: Click Yes if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
- **Client List**: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked **Yes** in the **Only allow specific IP** item.
- 3. Click **Apply**.

4.7.3 Firmware Upgrade

NOTE: Download the latest firmware from the ASUS website at <u>http://www.asus.com</u>

To upgrade the firmware:

- 1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Firmware Upgrade** tab.
- 2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
- 3. Click Upload.

NOTES:

- When the upgrade process is complete, wait for some time for the system to reboot.
- If the upgrade process fails, the wireless router automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly. To recover or restore the system, refer to section **5.2 Firmware Restoration**.

4.7.4 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

- From the navigation panel, go to Advanced Settings > Administration > Restore/Save/Upload Setting tab.
- 2. Select the tasks that you want to do:
 - To restore to the default factory settings, click **Restore**, and click **OK** in the confirmation message.
 - To save the current system settings, click **Save**, navigate to the folder where you intend to save the file and click **Save**.
 - To restore from a saved system settings file, click **Browse** to locate your file, then click **Upload**.

If issues occur, upload the latest firmware version and configure new settings. Do not restore the router to its default settings.

4.8 System Log

System Log contains your recorded network activities.

NOTE: System log resets when the router is rebooted or powered off.

To view your system log:

- From the navigation panel, go to Advanced Settings > System Log.
- 2. You can view your network activities in any of these tabs:
 - General Log
 - DHCP Leases
 - Wireless Log
 - Port Forwarding
 - Routing Table

/ISUS	Logout Reb	oot English 🔻
Quick Internet	Operation Mode: Wireless router	
General	General Log DHCP leases Wireles	s Log Port Forwarding Routing Table
品 Network Map	System Log - General Log This page shows the detailed system's act	Miles
🥂 Guest Network	System Time	Sat, Jan 01: 00:49:51: 2011
AiProtection	Uptime	0 days 0 hours 49 minutes 50 seconds
Adaptive QoS	Jan 1 00:31:27 kernel: ethJ: Broad Jan 1 00:31:27 kernel: device eth1	num BCH4331 802.11 Wiselers Controller 6.30.102.5 (#366174) num BCH4360 802.11 Wiselers Controller 6.30.302.5 (#366174) entered promieruous mode
USB Application	Jan 1 00:31:27 kernel: wir_phy_cal Jan 1 00:31:27 kernel: hr0: port 2 Jan 1 00:31:27 kernel: hr0: topolo	<pre>(ethl) estaring intening state init_scyby: NOT Implemented (shi) estaring learning taits py change detected, propagating</pre>
AiCloud 2.0	Jan 1 00:11:27 karnel: device eth2 Jan 1 00:31:27 kernel: he0: purt 3 Jan 1 00:31:27 kernel: he0: purt 3	<pre>(eth1) entering forwarding state entered promincums mode (eth2) entering lisening state (eth2) entering lawrning state</pre>
Advanced Settings	Jan 1 00:31:27 kernel: br0: port 4 Jan 1 00:31:27 kernel: br0: topolo	l entered promissions mode (v10.1) entering listening state gy change detected, propagating (schi) esturing (subwalling state
🚮 lan	Jan 1 00:31:27 kuttuli he0 topolo Jan 1 00:31:27 kuttuli he0 topolo Jan 1 00:31:35 dnamasq dhep(510) / Jan 1 00:31:85 dnamasq dhep(510) /	(vk0.1) entacing learning reats gridneg detected, propagating (vl0.1) entacing forwarding state microsofthir(bel) 192.100.1.0 et 6a.b?(00)06197 MICRAC(bel) 192.100.1.0 et 6a.b? (DECAC(bel) 192.100.1.0 et 6a.b?
💮 wan	Jan 1 00:32:12 dnamasg-Dop(510): 1 Jan 1 00:33:00 dnamasg-Dop(510): 1 Jan 1 00:33:00 dnamasg-Dop(510): 1	ENCORPERIENT(N=0) 192,148,1.197 10:N/:48.4e:N/:0 HECHARC(N=0) 192,148,1.197 10:N/:46:N/:60 LOUIE-CHAVEL HECHARCECTION 192,148,1.189 No:4e:Tl:4e:T':94 ENCONCECTION 192,148,1.189 No:4e:Tl:4e:T':94
🚳 19v6		DRCDWRDCHEF(beC) 152.169.1.3 Serid)(0:ber11:7d DRCDWRD(beC) 152.168.1.3 Serid)(0:f0:ber11:7d iFbinnets
🏀 VPN Server	Clear	
💟 Firewall		

5 Utilities

NOTES:

- Download and install the wireless router's utilities from the ASUS website:
 - Device Discovery v1.4.7.1 at <u>http://dlcdnet.asus.com/pub/ASUS/ LiveUpdate/Release/Wireless/Discovery.zip</u>
 - Firmware Restoration v1.9.0.4 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Rescue.zip</u>
 - Windows Printer Utility v1.0.5.5 at <u>http://dlcdnet.asus.com/pub/</u> <u>ASUS/LiveUpdate/Release/Wireless/Printer.zip</u>
- The utilities are not supported on MAC OS.

5.1 Device Discovery

Device Discovery is an ASUS WLAN utility that detects an ASUS wireless router device, and allows you to configure the wireless networking settings.

To launch the Device Discovery utility:

From your computer's desktop, click
 Start > All Programs > ASUS Utility > BRT-AC828/M2
 Wireless Router > Device Discovery.

NOTE: When you set the router to Access Point mode, you need to use Device Discovery to get the router's IP address.

5.2 Firmware Restoration

Firmware Restoration is used on an ASUS Wireless Router that failed during its firmware upgrading process. It uploads the firmware that you specify. The process takes about three to four minutes.

<u>F</u> ilename:	I		<u>B</u> rowse
Status After locating	the firmware file, click U	Jpload.	

IMPORTANT: Launch the rescue mode on the router before using the Firmware Restoration utility.

NOTE: This feature is not supported on MAC OS.

To launch the rescue mode and use the Firmware Restoration utility:

- 1. Unplug the wireless router from the power source.
- 2. Hold the Reset button at the rear panel and simultaneously replug the wireless router into the power source. Release the Reset button when the Power LED at the front panel flashes slowly, which indicates that the wireless router is in the rescue mode.

3. Set a static IP on your computer and use the following to set up your TCP/IP settings:

IP address: 192.168.1.x Subnet mask: 255.255.255.0

From your computer's desktop, click
 Start > All Programs > ASUS Utility BRT-AC828/M2
 Wireless Router > Firmware Restoration.

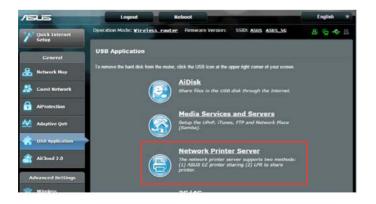
5. Specify a firmware file, then click **Upload**.

NOTE: This is not a firmware upgrade utility and cannot be used on a working ASUS Wireless Router. Normal firmware upgrades must be done through the web interface. Refer to **Chapter 4: Configuring the Advanced Settings** for more details.

5.3 Setting up your printer server

5.3.1 ASUS EZ Printer Sharing

ASUS EZ Printing Sharing utility allows you to connect a USB printer to your wireless router's USB port and set up the print server. This allows your network clients to print and scan files wirelessly.



NOTE: The print server function is supported on Windows® XP, Windows® Vista, and Windows® 7.

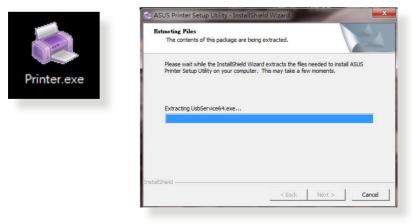
To set up the EZ Printer sharing mode:

- 1. From the navigation panel, go to **General** > **USB Application** > **Network Printer Server**.
- 2. Click **Download Now!** to download the network printer utility.

Quick Internet	Operation Mode: wireless rowter Firmware Version: SSID: ASUS ASUS_SG	8 6 4 8
General	Network Printer Server	5
🔒 Network Hap	The network printer server supports two methods. (1) ASUS EZ printer sharing (2) LPR to share printer.	
🔉 Guest Network	ASUS EZ printer sharing (Windows OS only) FAQ Download Now! Use LPR protocol to sharing printing FAQ (Windows)	
AiProtection	Use LPR protocol to sharing printing FAQ (MAC)	
Maptive QoS		
USB Application		

NOTE: Network printer utility is supported on Windows[®] XP, Windows[®] Vista, and Windows[®] 7 only. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

3. Unzip the downloaded file and click the Printer icon to run the network printer setup program.



4. Follow the onscreen instructions to set up your hardware, then click **Next**.

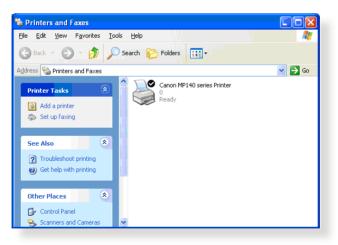


- 5. Wait a few minutes for the initial setup to finish. Click **Next**.
- 6. Click **Finish** to complete the installation.

7. Follow the Windows[®] OS instructions to install the printer driver.



8. After the printer's driver installation is complete, network clients can now use the printer.

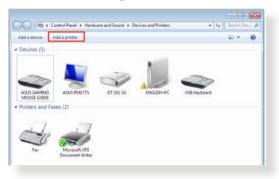


5.3.2 Using LPR to Share Printer

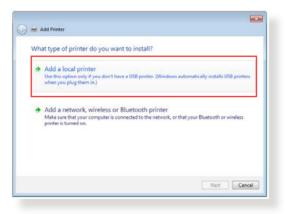
You can share your printer with computers running on Windows[®] and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

Sharing your LPR printer To share your LPR printer:

1. From the Windows[®] desktop, click **Start** > **Devices and Printers** > **Add a printer** to run the **Add Printer Wizard**.



2. Select Add a local printer and then click Next.



3. Select Create a new port then set Type of Port to Standard TCP/IP Port. Click New Port.

Choose a printer port	
A printer port is a type of cor	nnection that allows your computer to exchange information with a printer.
Use an existing port:	LPT1: (Printer Port)
Create a new port:	- 101
Type of port:	Standard TCP/IP Port
A server of the server	

4. In the **Hostname or IP address** field, key in the IP address of the wireless router then click **Next**.

🚱 🖶 Add Printer		×				
Type a printer hostname or IP address						
Device type:	TCP/IP Device	Ŧ				
Hostname or IP address:	192.168.1.1					
Port name:	192.168.1.1					
Query the printer and auto	Query the printer and automatically select the driver to use					
	Next	ancel				

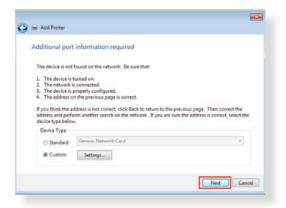
5. Select **Custom** then click **Settings**.



6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.

ort Settings	
Port Name:	192.168.1.1
Printer Name or IP Address:	192.168.1.1
Protocol	
Raw	LPR
Raw Settings	
Port Number:	9100
LPR Settings	
	LPRServer
LPR Byte Counting Enab	bled
SNMP Status Enabled	
Community Name:	public
SNMP Device Index:	1
	OK Cano

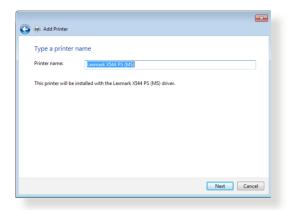
7. Click Next to finish setting up the standard TCP/IP port.



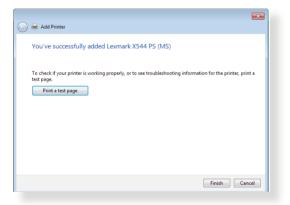
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.

install the printer dr	iver		
Choose your pri	nter from the list. Click	Windows Update to see more mod	els.
To install the dri	ver from an installation	CD, click Have Disk.	
Manufacturer	* Printers		*
Kyocera	Lem	ark: X422 (MS)	
Lanier		ark: X543 P5 (MS)	
Lexmark		ark X544 PS (MS)	. (3)
Microsoft		ark X642e (M5)	-
This driver is digitally		Windows Update	Have Disk_
	and the owned		

9. Click **Next** to accept the default name for the printer.



10. Click **Finish** to complete the installation.



5.4 Download Master

Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

NOTE: You need a USB device connected to the wireless router to use Download Master.

To use Download Master:

1. Click **General** > **USB application** > **Download Master** to download and install the utility automatically.

NOTE: If you have more than one USB drive, select the USB device you want to download the files to.

- 2. After the download process is finished, click the Download Master icon to start using the utility.
- 3. Click Add to add a download task.



4. Select a download type such as BitTorrent, HTTP, or FTP. Provide a torrent file or a URL to begin downloading.

NOTE: For details on Bit Torrent, refer to section **5.4.1 Configuring the Bit Torrent download settings**.

5. Use the navigation panel to configure the advanced settings.



5.4.1 Configuring Bit Torrent download settings

/ISUS					
Task	Bit Torrent Setting				
🚋 Task	Port				
Settings	Use the default port Use the following port				
Seneral	Incoming port Opend Limits:				
Rit Torrest	Maximum download speed.	KEVS NEVS			
	Difforment Network setting				
X N20	Difforrent protocol encryption	Encryption disabled			
	Max peers allowed performent	100 Enutife CHT to activate trackless forrent download			
	DHT network				
	Apply				

To configure BitTorrent download settings:

- 1. From Download Master's navigation panel, click **Bit Torrent** to launch the **Bit Torrent Setting** page.
- 2. Select a specific port for your download task.
- 3. To prevent network congestion, you can limit the maximum upload and download speeds under **Speed Limits**.
- 4. You can limit the maximum number of allowed peers and enable or disable file encryption during downloads.

5.4.2 NZB settings

You can set up a USENET server to download NZB files. After entering USENET settings, **Apply**.

Task	STATE AND A STATE	
Task	NZB Setting	
Task	Setup USENET server to download NZB tiles:	
Settings	USENET Server	
	USENET Server Port	119
General	Maximum download speed	d Kas
Bit Torrent	SSL/TLS connection only	
	User name	
NZIS	Password	
	Confirm Password	•
	Number of connections per NZB tasks	2
		Apply

6 Troubleshooting

This chapter provides solutions for issues you may encounter with your router. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at:

<u>http://support.asus.com/</u> for more product information and contact details of ASUS Technical Support.

6.1 Basic Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

Upgrade Firmware to the latest version.

- Launch the Web GUI. Go to Advanced Settings > Administration > Firmware Upgrade tab. Click Check to verify if the latest firmware is available.
- 2. If the latest firmware is available, visit the ASUS global website at <u>http://www.asus.com/Networks/Wireless_Routers/BRTAC828/M2/#download</u> to download the latest firmware.
- 3. From the **Firmware Upgrade** page, click **Browse** to locate the firmware file.
- 4. Click **Upload** to upgrade the firmware.

Restart your network in the following sequence:

- 1. Turn off the modem.
- 2. Unplug the modem.
- 3. Turn off the router and computers.
- 4. Plug in the modem.
- 5. Turn on the modem and then wait for 2 minutes.
- 6. Turn on the router and then wait for 2 minutes.
- 7. Turn on computers.

Check if your Ethernet cables are plugged properly.

- When the Ethernet cable connecting the router with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your powered-on computer with the router is plugged in properly, the corresponding LAN LED will be on.

Check if the wireless setting on your computer matches that of your computer.

 When you connect your computer to the router wirelessly, ensure that the SSID (wireless network name), encryption mehtod, and password are correct.

Check if your network settings are correct.

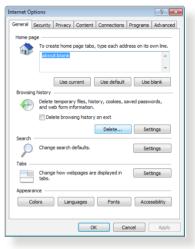
- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless router's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the web GUI, Network Map > Clients page, and hover the mouse pointer over your device in Client Status.



6.2 Frequently Asked Questions (FAQs)

I cannot access the router GUI using a web browser

- If your computer is wired, check the Ethernet cable connection and LED status as described in the previous section.
- Ensure that you are using the correct login information. The default factory login name and password is "admin/admin". Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer 8, follow these steps:
 - Launch Internet Explorer 8, then click Tools > Internet Options.
 - 2. In the General tab, under Browsing history, click Delete..., select Temporary Internet Files and Cookies then click Delete.



NOTES:

- The commands for deleting cookies and files vary with web browsers.
- Disable proxy server settings, cancel the dial-up connection, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to Chapter 1 of this user manual.
- Ensure that you use CAT5e or CAT6 ethernet cables.

The client cannot establish a wireless connection with the router.

NOTE: If you are having issues connecting to 5Ghz network, make sure that your wireless device supports 5Ghz or features dual band capabilities.

• Out of Range:

- Move the router closer to the wireless client.
- Try to adjust antennas of the router to the best direction as described in section **1.4 Positioning your router**.

• DHCP server has been disabled:

- Launch the web GUI. Go to General > Network Map> Clients and search for the device that you want to connect to the router.
- If you cannot find the device in the Network Map, go to Advanced Settings > LAN > DHCP Server, Basic Config list, select Yes on the Enable the DHCP Server.

/505	Logout Reboo		English 🔻		
Quick Internet Setup	Operation Mode: Wireless router Fi	rmware Version: SSID: <u>ASUS ASUS 356</u> Switch Control	8645		
General					
🐣 Network Map	LAN - DHCP Server				
😹 Guest Network	DHCP [Dynamic Hist Configuration Printco)] is a protocol for the automatic configuration used on IP intervets. The DHCP server can assign each client an IP address and informs the client of the of DHC server IP and delaut gateway IP isarwal Tuy. Assigned: IP: account the direct Tist (Tist: Tist(Tist. Tist(Tist.)). FAG				
AiProtection	Besic Config				
Magetive QuS	Enable the OHOP Server	O Yas 🔍 No	1		
	Router's Domain Name				
USB Application	IP Pool Starting Address		- D		
AiCloud 2.0	IP Pool Ending Address				
Advanced Settings	Lease Time				
💝 Wireless	Default Gateway				
	ONS and WINS Server Setting		1		
G 140	DNS Server		Ť.		
😳 WAN	WINS Server				
😝 19v6	Enable Manual Assignment		1		
VPN Server	Enable Manual Assignment	• Yes O No	ļ.		
	Manually Assigned IP annual the DNCP Institut Invet.32)				
V Firewall	MAC address	P Address	Add/Delete		
Administration			•		
System Log					
		Apply			

 SSID has been hidden. If your device can find SSIDs from other routers but cannot find your router's SSID, go to Advanced Settings > Wireless > General, select No on Hide SSID, and select Auto on Control Channel.

/ISUS	Logout Rebo	K English 🔻
Quick Internet Setup	Operation Mode: <u>Wireless Fouter</u> F	irmware Version: SSID: <u>ASUS ASUS_SG</u> <u>B</u> <u>C</u> <u>C</u> <u>C</u> .C Filter RADIUS Setting Professional
General	Wireless - General	
😹 Guest Network	Set up the wireless related information below Frequency	2.490 •
AlProtection	59D	ASUS
Maptive QoS	Hide SSID	● Yes O No
🔹 USB Application	Wireless Mode	Auto Zi big Protection
AiCloud 2.0	Channel bandwidth	20/40 99:2
C	Control Channel	Auto -
Advanced Settings	Authentication Method	Open System
windess	WEP Encryption	kone
🕼 lan		Αμοίγ

- If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. If not, adjust the channel, channel bandwidth, and wireless mode.
- If you still cannot connect to the router wirelessly, you can reset your router to factory default settings. In the router GUI,click Administration > Restore/Save/Upload Setting and click Restore.

/sus	Logout	Reboot			English
guick Internet	Operation Mode: Wireles	router Firmware	Version:	SSID: ASUS ASUS_SG	8 6 4 5
Setup	Operation Mode System	Firmware Upgrade	Restore	/Save/Upload Setting	
General	anna anna anna anna	-			
🔒 Network Map	Administration - Resto				
28 Guest Network	This function allows you to sa	we current settings of Ro	uter to a Ni	e, or load settings from a file.	
ALC: SUCCESSION	Factory default		estore		
AlProtection	Gave setting		Save		
Adaptive QoS	Restore setting		pload	Choose File No Sie chosen	
dist Application					
AiCloud 2.0					

Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to General> Network Map, and check the Internet Status.
- If your router cannot connect to your ISP's WAN IP address, try restarting your network as described in the section **Restart your network in following sequence** under **Basic Troubleshooting**.



- The device has been blocked via the Parental Control function. Go to General > Parental Control and see if the device is in the list. If the device is listed under Client Name, remove the device using the Delete button or adjust the Time Management Settings.
- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.
- Check the status indicators on the ADSL modem and the wireless router. If the WAN LED on the wireless router is not ON, check if all cables are plugged properly.

You forgot the SSID (network name) or network password

- Setup a new SSID and encryption key via a wired connection (Ethernet cable). Launch the web GUI, go to **Network Map**, click the router icon, enter a new SSID and encryption key, and then click **Apply**.
- Reset your router to the default settings. Launch the web GUI, go to Administration > Restore/Save/Upload Setting, and click Restore. The default login account and password are both "admin".

How to restore the system to its default settings?

 Go to Administration > Restore/Save/Upload Setting, and click Restore.

The following are the factory default settings:

User Name:	admin
Password:	admin
Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	192.168.1.1
Domain Name:	(Blank)
Subnet Mask:	255.255.255.0
DNS Server 1:	192.168.1.1
DNS Server 2:	(Blank)
SSID (2.4GHz):	ASUS
SSID (5GHz):	ASUS_5G

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **5.2 Firmware Restoration** on how to use the Firmware Restoration utility.

Cannot access Web GUI

Before configuring your wireless router, do the steps described in this section for your host computer and network clients.

A. Disable the proxy server, if enabled.

Windows[°] 7

- 1. Click **Start > Internet Explorer** to launch the browser.
- Click Tools > Internet options > Connections tab > LAN settings.



- From the Local Area Network (LAN) Settings screen, untick Use a proxy server for your LAN.
- 4. Click **OK** when done.

Automatically detect settings Use automatic configuration script Address oxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: B0 Advanced		nfiguration	may override man lisable automatic		gs. To ensure the ion.
Address	Automatic	ally detect s	ettings		
oxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: 80 Advanced	Use autom	natic configu	ration script		
oxy server Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: 80 Advanced	address				7
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: Port: 80 Advanced					
dial-up or VPN connections). Address: Port: 80 Advanced	ovy cerver				
	oxy server				
The second second for local addresses	Use a prop			e settings	will not apply to
Bypass proxy server for local addresses	Use a prop dial-up or		tions).		
	Use a prop dial-up or Address:	VPN connec	tions).	80	
QK Cance	Use a prop dial-up or Address:	VPN connec	tions).	80	

MAC OS

- From your Safari browser, click Safari
 Preferences > Advanced > Change Settings...
- From the Network screen, deselect FTP Proxy and Web Proxy (HTTP).
- 3. Cllick **Apply Now** when done.

		Locatio	on: Auton	natic	:	3	
		She	w: Built-i	n Ethernet		9	
	-0	TCP/IP	PPPoE /	ppleTalk Pro	ixies Ether	met	
Selec	t a proxy	server to	configure:	FTP Pro	oxy Server		
-	FTP Proxy			8			
	Web Proxy			Pro	cy server req	uires passwo	rd
		b Proxy (H Proxy (RT)		U	Set Passe	(brow	
8	SOCKS Pro	жу		Ę.	Contrain	iona	
-	Copher Pr			+			
		settings fo Domains:					
-							

NOTE: Refer to your browser's help feature for details on disabling the proxy server.

B. Set the TCP/IP settings to automatically obtain an IP address.

Windows[°] 7

- 1. Click Start > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections.
- 2. Select Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), then click Properties.

Networking Authenticatio	n	
Connect using:		
Realtek PCle GBE	Family Controller	
	1	Configure
This connection uses the	following items:	Configure
Client for Micros	oft Networks	
🗹 📕 QoS Packet Sci		
	Sharing for Microsoft Netv	vorks
	6.X SPR Protocol Driver	
Internet Protoco	Version 6 (TCP/IPv6)	
	Version 4 (TCP/IPv4)	TTT BOVAR
🗹 🛥 Link-Layer Topo	I Vesion 4 (TCP/IPv4) logy Discovery Mapper 1/ logy Discovery Responde	
Link-Layer Topo Link-Layer Topo	logy Discovery Mapper 1/ logy Discovery Responde	er
 ✓ → Link-Layer Topo ✓ → Link-Layer Topo Instal 	logy Discovery Mapper I/	
A Link-Layer Topo A Link-Layer Topo Install Description	logy Discovery Mapper D logy Discovery Responde Uninstall	er Properties
Link-Layer Topo Link-Layer Topo Link-Layer Topo Instal Description Transmission Control F wide area network pro	Nogy Discovery Mappen // Nogy Discovery Responde Uninstall Protocol/Internet Protocol. tocol that provides comm	Properties
Link-Layer Topo Link-Layer Topo Link-Layer Topo Instal Description Transmission Control F	Nogy Discovery Mappen // Nogy Discovery Responde Uninstall Protocol/Internet Protocol. tocol that provides comm	Properties
Link-Layer Topo Link-Layer Topo Link-Layer Topo Instal Description Transmission Control F wide area network pro	Nogy Discovery Mappen // Nogy Discovery Responde Uninstall Protocol/Internet Protocol. tocol that provides comm	Properties
Link-Layer Topo Link-Layer Topo Link-Layer Topo Instal Description Transmission Control F wide area network pro	Nogy Discovery Mappen // Nogy Discovery Responde Uninstall Protocol/Internet Protocol. tocol that provides comm	Properties
Link-Layer Topo Link-Layer Topo Link-Layer Topo Instal Description Transmission Control F wide area network pro	Nogy Discovery Mappen // Nogy Discovery Responde Uninstall Protocol/Internet Protocol. tocol that provides comm	Properties

3. To obtain the IPv4 IP settings automatically, tick **Obtain an IP address automatically**.

> To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

4. Click **OK** when done.

neral Alt	ernate Configuration				
nis capabil	t IP settings assigned auto ity. Otherwise, you need t ropriate IP settings.				
Obtair	n an IP address automatica	ally			
🔘 Use th	e following IP address:				
IP addre	55:				
Subnet r	nask:	к. К.	1		
Default (gateway:	÷.	1.	4	
() Obtair	DNS server address auto	matically			
O Use th	e following DNS server ad	dresses:			
Preferre	d DNS server:				
Alternati	e DNS server:	80			
Valida	ate settings upon exit			Adva	inced

MAC OS

- Click the Apple icon located on the top left of your screen.
- Click System Preferences > Network > Configure...
- 3. From the **TCP/IP** tab, select **Using DHCP** in the **Configure IPv4** dropdown list.
- 4. Cllick **Apply Now** when done.

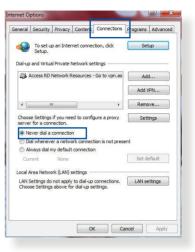
Show All	Displays Sou	nd Network	Startup De	sk		
	L	cation: A	utomatic		•	
		Show: B	ailt-in Eth	ernet	•	
	TCP/	IP PPPoE	Apple1	alk Proxies	Ethernet	
Conf	igure IPv4:	Using DH	CP		•	
1	P Address:	192.168.1	82.103		Renew DHO	Please
Sul	bnet Mask:	255.255.2	55.0	DHCP Client	ID: Of required)	
	Router:	192.168.1	82.250		on redones.	
D	NS Servers:	192.168.1	28.10			(Optional)
Search	Domains:	_				(Optional)
IPv	6 Address:	fe80:0000:	0000:000	D:0211:24ff:fe3	2:b18e	
		Configure	IPv6.			(?)

NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

C. Disable the dial-up connection, if enabled.

Windows[°] 7

- 1. Click **Start** > **Internet Explorer** to launch the browser.
- 2. Click Tools > Internet options > Connections tab.
- 3. Tick **Never dial a connection**.
- 4. Click OK when done.



NOTE: Refer to your browser's help feature for details on disabling the dial-up connection.

Appendices

Notices

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <u>http://csr.asus.com/english/Takeback.htm</u> for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

IMPORTANT! This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

WARNING!

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- Users must not modify this device. Modifications by anyone other than the party responsible for compliance with the rules of the Federal Communications Commission (FCC) may void the authority granted under FCC regulations to operate this device.
- For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements - Article 3

Protection requirements for health and safety – Article 3.1a Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

Operate the device in 5150-5250 MHz frequency band for indoor use only.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 31 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

WARNING!

- This radio transmitter (3568A-RT0V00) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.
- Le présent émetteur radio (3568A-RT0V00) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.
- For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.
- The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

NCC 警語

經型式認證合格之低功率射頻電機,非經許可,公司、商號或 使用者均不得擅自變更頻率、加大功率或變更原設計之特性及 功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通 信;經發現有干擾現象時,應立即停用,並改善至無干擾時方 得繼續使用。前項合法通信,指依電信法規定作業之無線電通 信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電 波輻射性電機設備之干擾。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free

Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making

the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the

terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machinereadable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

- 6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
- 7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- 8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- 9. The Free Software Foundation may publish revised and/ or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.

Tel. No.:	+90 212 3311000
Address:	AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
	AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.:	+90 212 3567070
Address:	CEMAL SURURI CD. HALIM MERIC IS MERKEZI
	No: 15/C D:5-6 34394 MECIDIYEKOY/
	ISTANBUL

KOYUNCU ELEKTRONIK BILGI ISLEM SIST. SAN. VE DIS TIC. A.S.

Tel. No.:	+90 216 5288888
-----------	-----------------

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

ASUS Contact information

ASUSTeK COMPUTER INC. (Asia Pacific)

Address15 Li-Te Road, Peitou, Taipei, Taiwan 11259Websitewww.asus.com.tw

Technical Support

Telephone	+886228943447
Support Fax	+886228907698
Online support	support.asus.com

ASUS COMPUTER INTERNATIONAL (America)

Address	800 Corporate Way, Fremont, CA 94539, USA	
Telephone	+15107393777	
Fax	+15106084555	
Website	usa.asus.com	
Online support	support.asus.com	

ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkort Str. 21-23, D-40880 Ratingen, Germany
Support Fax	+49-2102-959931
Website	asus.com/de
Online contact	eu-rma.asus.com/sales

Technical Support

Telephone (Component)	+49-2102-5789555
Telephone Germany	
(System/Notebook/Eee/LCD)	+49-2102-5789557
Telephone Austria	
(System/Notebook/Eee/LCD)	+43-820-240513
Support Fax	+49-2102-959911
Online support	support.asus.com

Networks Global Hotline Information

Region	Country	Hotline Number	Service Hours
	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
		0049-1805010920	
	Germany	0049-1805010923	09:00-18:00 Mon-Fri
	Germany	(component support)	10:00-17:00 Mon-Fri
		0049-2102959911 (Fax)	
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
Europe	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	+46-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	+44-1442265548	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Region	Country	Hotline Numbers	Service Hours
	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri
		0600-1252/6/	09:00-17:00 Sat-Sun
		0081-570783886	09:00-18:00 Mon-Fri
		(Non-Toll Free)	09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717	09:00-18:00 Mon-Fri
		1800-8525201	
	Singapore	0065-64157917	11:00-19:00 Mon-Fri
Asia-Pacific		0065-67203835	11:00-19:00 Mon-Fri
		(Repair Status Only)	11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
	India(WL/NW)	1000-2090303	09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000	09:30-17:00 Mon-Fri
		500128 (Local Only)	9:30 – 12:00 Sat
	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
Americas	Canada	1-012-202-2/0/	9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri
			08:00-15:00 CST Sat

Networks Global Hotline Information

Deview	C		C - mail - a 11
Region	Country	Hotline Numbers	Service Hours
	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
Middle	UAE	00971-42958941	09:00-18:00 Sun-Thu
East +	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
Africa	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
Balkan		00359-29889170	09:30-18:00 Mon-Fri
Countries	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400	00.00.16.00 Mars Eri
		00368-59045401	08:00-16:00 Mon-Fri
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

Networks Global Hotline Information

NOTE: For more information, visit the ASUS support site at: <u>http://support.asus.com</u>

Manufacturer:	ASUSTeK Computer Inc.	
	Tel:	+886-2-2894-3447
	Address:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Authorised	ASUS Computer GmbH	
representative in Europe:	Address:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY